GnuPG VS-Desktop®

Krypto-Schutz für die
Mail- und Datenverschlüsselung

g10 Code GmbH ▪ Gutenbergweg 4 ▪ 40699 Erkrath / Germany ▪ +49 2104 493 879 0 ▪ info@gnupg.com ▪ www.gnupg.com

Die sicherste Art der digitalen Kommunikation

Bewährt und sicher

Seit 1997 funktioniert der *„GnuPG-Verschlüsselungscode“* und bietet einen unerreichten Schutz vor Nachrichtenüberwachung und unberechtigter Datenspeicherung durch Dritte. Ein Code von dem es heißt, dass es selbst der National Security Agency (NSA) bis heute nicht gelungen ist, diesen zu entschlüsseln:

```
-----BEGIN PGP MESSAGE-----

kA0DAAgW4/3/IY5FtysBy11iAF9Q3S8KCkdudVBHIC0gZGllIHNpY2hlcnN0ZSBB
cnQgZGVyIE5hY2hyaWNodGVuw7xiZXJ0cmFndW5nCgpXZWl0ZXJlIGluZm9zOiB3
d3cuZ251cGcuY29tCgqJAfUEABYIAZ0WIQTB00tpIZ5K7sC6HCHj/f8hjkW3KwUC
X1DdL8C+JgCYMwRU5NYCFgkrBgEEAdpHDwEBB0D16DIBI1sikMsiN5rSt/gjzms6
ZT7KU25dh0+e5wn8zbQnV2VybmVyIEtvY2ggKHdoZWF0c3RvbmUgY29tbWl0IHNp
Z25pbmcpiH8EExYIACcFAlTk1gICGwMFCRLMAwAFCwkIBwIGFQgJCgsCBBYCAwEC
HgECF4AACgkQ4/3/IY5FtytAcgD/TaGyWy+kCd2A3s6/wew9LQx1fcEejlHQrkYS
MC6RrN4BAJdNgnoEqIdiGZIgf5TsGl+wj9Qhycrrn0ljrSBfxEkAuDgEVsB9QhIK
KwYBBAGXVQEFAQEHQLKYNXqUd9d/MQYvfGMO+EBndtcW6lYBAtD0sFMkq9JdAwEI
B4hhBBgWCAAJBQJWwH1CAhsMAAoJEOP9/yGORbcrP9AA/0Rbr/THO9LVhqiOk/RI
6vYRd6N5yWINECw5vnTXTZkiAP9m2/gdOTSRvVjSNaIRAMXU1ggrSEGt1l730gJq
auNdCAAKCRDj/f8hjkW3K0A8AP4r+D4pM/YTX74/b7OOmr2oz/xvXBaXgKFnjiUf
hPS3lQEA9t3o0N1TAeTdC1A6pKRxgriCM1Bfu2KSTOi6qlXS5Ao=
-----END PGP MESSAGE-----
```

Made in Germany
Unsere IT-Sicherheits-Software entsteht in Deutschland – alle Leistungen erhalten Sie direkt vom Hersteller

Erfahrung schafft Vertrauen

Unsere Krypto-Software entsteht in einem offenen und transparenten Entwicklungsprozess. Mit viel Herz, großer Freude und Leidenschaft arbeiten wir Tag für Tag kontinuierlich für Millionen Nutzer weltweit am maximalen Privatsphärenschutz bei der Nachrichten- und Datenübertragung.

Die universelle Krypto-Komplettlösung

Die Situation

Jede digitale Nachricht durchläuft bei der Übermittlung viele Computer und landet oftmals unberechtigt in fremden Datenbanken.

Die Lösung

Um sicherzustellen, dass vertrauliche Nachrichten nicht mitgelesen werden können, erhalten Sie von uns eine für den VS-NfD Einsatz zugelassene Komplettlösung zum Verschlüsseln und Signieren von Mails und Daten. Darüber hinaus enthält unser Gesamtprogramm individuelle Service-, Schulungs- und Supportleistungen im Rahmen einer vertraglichen Vereinbarung:

- **IT-Sicherheits-Software**
  Open Source Softwarepaket bestehend aus Krypto-Backend, Zertifikatsmanager und PlugIns.
- **Support und Maintenance**
  Telefonischer Support, Sicherheits- und Major-Updates direkt von den leitenden Entwicklern.
- **Schulung und Beratung**
  Individuelle Herstellerberatung mit Einführungs- und Schulungskursen für Ihre Administratoren und IT-Sicherheitsbeauftragten.

Krypto-Alleskönner

Wir schützen Ihre Kommunikation indem wir Ihnen eine programmübergreifende *„Ende-zu-Ende Verschlüsselung“* ermöglichen, mit der Sie sowohl Mails, Daten und Textnachrichten ver- und entschlüsseln, als auch digitale Signaturen erzeugen und prüfen können:

- **Mails und Anhänge**
  Handhaben Sie Krypto-Mails so unkompliziert wie Standard-Mails über Ihre Outlook-Oberfläche.
- **Dateien und Ordner**
  Verschlüsseln Sie Dateien jeden Formats und Ordner jeder Datengröße über das Explorer-Menü.
- **Chats und Messenger**
  Kommunizieren Sie verschlüsselt in allen Chat-, Messenger- und Meeting-Diensten.
- **Cloud- und Filesharing**
  Archivieren, transferieren oder hosten Sie große Datenmengen im Krypto-Format.
- **Zertifikats- und Schlüsselverwaltung**
  Nutzen Sie die Möglichkeiten der automatisierten Zertifikats- und Schlüsselverwaltung.

Sichere Kommunikation

GnuPG VS-Desktop® verhindert das Mitlesen Ihrer digitalen Kommunikation und in der Cloud gespeicherter Daten durch Dritte, einschließlich Telekommunikationsanbieter und staatlicher Stellen. Selbst wenn Ihre verschlüsselten Mails auf dem Übertragungsweg abgefangen und gespeichert werden sollten, bleiben diese für Unautorisierte unmöglich zu entschlüsseln.

IT-Sicherheits-Software für Behörden und Institutionen

Volle Transparenz

GnuPG VS-Desktop® ist ein Open Source Softwarepaket und besteht aus unabhängig entwickelten Programmen. Es beinhaltet als Basis den Kryptokern *„GnuPG“* in dem jeweils vom BSI zugelassenen Konstruktionsstand, den Schlüssel- und Zertifikatsmanager *„Kleopatra“* sowie den PlugIns *„GpgOL“* und *„GpgEX“* für die Mail- und Datenverschlüsselung.

Funktionsvorteile

Wir vereinheitlichen die beiden Verschlüsselungsprotokolle *„OpenPGP“* und *„S/MIME“* zu einer flexiblen Komplettlösung. Im Gegensatz zu einer Transport- oder Gateway-Verschlüsselung macht es die Ende-zu-Ende Verschlüsselung unmöglich, Mails auf dem Übertragungsweg zu entschlüsseln bzw. zu lesen. Es besteht daher keine Notwendigkeit mehr den Übertragungsweg selbst abzusichern – auch außerhalb Ihres Netzwerks und ohne VPN kommunizieren Sie mit uns stets sicher:

- Die Nachrichten können nur von den jeweiligen Endpunkten entschlüsselt werden.
- Die Echtheit des Kommunikationspartners kann jederzeit gewährleistet werden.
- Der Inhalt einer Nachricht kann nicht unbemerkt verändert oder ausgetauscht werden.

Sicherheit mit VS-NfD Freigabe

Bereits in 2019 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) unsere Krypto-Komplettlösung für die Übertragung von vertraulichen Dokumenten der Geheimhaltungsstufe *„Verschlusssache – nur für den Dienstgebrauch“* zugelassen. Diese gilt sowohl für das OpenPGP- als auch für das S/MIME-Protokoll und sieht vor, dass Langzeitgeheimnisse u.a. auch auf der Festplatte gespeichert werden können. Bei Geheimhaltungsgraden die über VS-NfD hinausgehen, kann der Einsatz unserer Software direkt mit dem BSI geklärt werden.

Der neue Weg

Die Zulassung der Verschlüsselungssoftware *„Chiasmus“* läuft am 31.12.2021 endgültig ab. Alle Behörden und Institutionen die bislang auf diese Software angewiesen waren und VS-NfD Daten verschlüsselt haben, sind nun in der Pflicht auf andere zugelassene Lösungen umzustellen. Durch die BSI-Zulassung kann GnuPG VS-Desktop® diese bisher verwendete Verschlüsselungs-Software ersetzen.

Anwendungsvorteile

- Nutzung aller digitalen Übertragungswege
- Automatisierte Schlüsselverwaltung mit Aktualisierung
- Nutzerfreundliche Outlook- und Explorer-Integration

Funktionsprinzip

Bereits vor der Datenübermittlung verschlüsselt der *„Sender“* seine digitalen Informationen mit dem öffentlichen Schlüssel der Person, die sich am Endpunkt der Kommunikation befindet. Einzig der *„Empfänger“* ist in der Lage, die erhaltenen Informationen mittels seines dazugehörigen privaten Schlüssels zu entschlüsseln.

Verschlüsselte Kommunikation im vertrauten Arbeitsumfeld

Maximale Usability

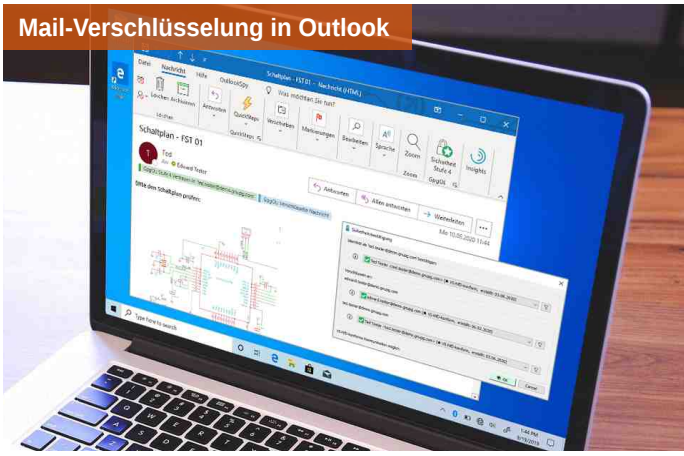
Unser Ziel ist, dass sich verschlüsselte Kommunikation so anfühlt, wie über den herkömmlichen Weg. Dafür arbeiten wir täglich mit grossem Eifer an Lösungen, die in Ihren Arbeitsalltag einfließen und Sie unterstützen:

- **Mail-Verschlüsselung**
  Wir integrieren die Ende-zu-Ende Verschlüsselung direkt in Ihre vertraute Outlook-Oberfläche und ermöglichen Ihnen somit den einfachsten Umgang mit Krypto-Mails. Der Abruf von vertrauenswürdigen Zertifikaten erfolgt dabei automatisch im Hintergrund ohne die gewohnten Arbeitsabläufe zu belasten.

- **Daten-Verschlüsselung**
  Wir erweitert Ihren vertrauten Explorer um die Möglichkeit, Dateien und Ordner mit nur wenigen Klicks zu ver- und entschlüsseln. Der verschlüsselte Datenaustausch kann so auch über ungesicherte Filesharing-Dienste erfolgen, die über keine eigene VS-NfD Zulassung verfügen.

- **Text-Verschlüsselung**
  Wir stellen Ihnen einen Krypto-Notizblock zur Verfügung, mit dem Sie Nachrichten, Texte, Passwörter etc. blitzschnell ver- und entschlüsseln können. Der zusätzliche Einsatz eines Mailprogramms ist dazu nicht erforderlich.

Mail-Verschlüsselung in Outlook



Datei-Verschlüsselung über den Explorer

Text-Verschlüsselung über den Krypto-Notizblock

Multifunktionale Anwendung

Durch die modulare Architektur kann unsere Sicherheits-Software leicht in alle etablierten Anwendungen integriert werden. Wir nutzen ausschließlich offene Standards und Normen und ermöglichen Ihnen damit eine programmübergreifende Interoperabilität. Alle gängigen Algorithmen zur Verschlüsselung und Authentifizierung werden mit uns unterstützt.

Identitätsmanagement und Vertrauensstufen

Identitätsmanagement

Kryptographisches Material ist immer mit einer Identität verbunden. Die Kombination aus Schlüssel- und Identitätsinformation wird als öffentlicher Schlüssel bzw. Zertifikat bezeichnet. GnuPG VS-Desktop® bietet Ihnen die Möglichkeit, diese für die Kommunikation notwendigen Zertifikate automatisiert auszutauschen.

Dank kryptographischer Signaturen ist es stets möglich sicherzustellen, ob der Kommunikationspartner auch wirklich authentisch ist. Unser Outlook-PlugIn verwendet unterschiedliche *„Vertrauensstufen“* zum Validieren und Authentifizieren Ihrer Kommunikationspartner, womit sich organisatorische Maßnahmen einfach darstellen lassen:

Unterstützte Algorithmen

- **S/MIME**
  Bei S/MIME werden Schlüssel lokal erstellt und durch eine zentrale Instanz (Certificate Authority) beglaubigt. Diese kann wiederum andere Instanzen beglaubigen, wodurch eine hierarchische Vertrauenskette entsteht.

- **OpenPGP**
  Bei OpenPGP werden Schlüssel lokal erstellt und von Ihren Kommunikationspartnern beglaubigt. Es gibt keine zentrale Beglaubigungsinstanz – jeder Nutzer erstellt sich sein eigenes Netz des Vertrauens über das Beglaubigen anderer Schlüsselpaare durch sein eigenes Zertifikat.

Sicherheit	Einstufung	Beschreibung
Stufe 0	Keine Validierung	Der Schlüssel des Kommunikationspartners ist unbekannt.
Stufe 1	Validierung über Mail-Adresse	Unser Outlook-PlugIn trifft hier keine Vertrauensaussagen über die Identität des Absenders, verwendet aber den Schlüssel zur Verschlüsselung. Diese Stufe schützt vor passiven Angreifern, jedoch nicht vor aktiven *„Man in the Middle“*-Angriffen.
Stufe 2	Eingeschränkte Identitätsprüfung	Der Schlüssel wurde vom Provider automatisch über HTTPS ausgeliefert. Das geht nur, wenn dieser das Web Key Directory einsetzt. Es besteht also ein Grundvertrauen, dass der Absender die Mailadresse kontrolliert, von der aus die Nachricht gesendet wurde.
Stufe 3	Validierung über Mail-Adresse	Diese Stufe schützt vor aktiven Angreifern, d.h. dass eine *„Third Party"* diesen Schlüssel mit einem vertrauenswürdigen Wurzelzertifikat beglaubigt hat.
Stufe 4	Validierung über Zertifizierungsstelle	Sie selbst oder eine ultimativ vertrauenswürdige Person haben den Fingerabdruck des Schlüssels geprüft und diesen direkt signiert.

Prozessbegleitung

Erfahrungsgemäß kann es bei der Krypto-Kommunikation aufgrund fehlender Zertifikate oder ungültiger Signaturen gelegentlich zu Problemen kommen – als Hersteller, Maintainer und Dienstleister stehen wir Ihren Administratoren und IT-Sicherheitsbeauftragten jederzeit mit Rat und Tat zur Seite.

Bedarfsoptimierte Software-Paketierung

Software-Paketierung

Damit sich GnuPG VS-Desktop® direkt in die Arbeitsumgebung der Nutzer einbindet und u.a. vollautomatisch Entscheidungen über das Vertrauen in Zertifikate treffen kann, bekommt jeder Kunde für seine Organisation die passende Lösung.

Wahlweise entscheiden sich unsere Kunden entweder für unsere Standard-MSI-Paketierung oder für ein individuell vorkonfiguriertes und auf die Bedürfnisse Ihrer Organisation abgestimmtes Installationspaket:

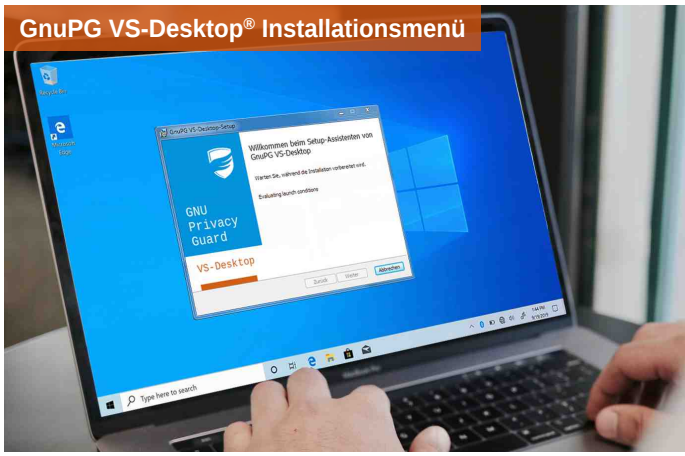
- Die Vertrauensanker können vorab festgelegt und vorkonfiguriert werden.
- Die Funktionsauswahl der Benutzeroberfläche kann nutzerspezifisch angepasst werden.
- Der Zertifikats- und Sperrlistenabruf kann über LDAP / Active Directory erfolgen.

Bereits vor der Installation können Sie festlegen, welchen Zertifizierungsstellen das Vertrauen für Ihre internen und externen Zertifikate erteilt werden soll. Ebenso kann die Nutzeroberfläche auf ein Minimum reduziert werden, wodurch die administrativen Einstellungen unverändert bleiben. Somit kann gewährleistet werden, dass sich jeder Nutzer auf einem VS-NfD konformen Schutzniveau befindet, ohne sich mit komplexen Details auseinander-setzen zu müssen.

Einbindung externer Partner

Wenn sowohl innerhalb als auch außerhalb von Institutionen mit externen Partnern kommuniziert werden soll, haben Sie mit uns die Möglichkeit Ihre Paketierung entsprechend den erworbenen Nutzerzahlen auch weiterzugeben. Durch die einheitliche Paketierung entfällt eine nachträgliche Konfiguration und es kann sofort und ohne Austausch eines Passworts VS-NfD konform kommuniziert werden. Stillstände von Arbeits-gruppen aufgrund fehlender Ende-zu-Ende Verschlüsselung sind dadurch ausgeschlossen.

Installieren und loslegen
Ihre Partner benötigen nur Ihr Installationspaket, eine Smartcard und die dazugehörige PIN



Smartcard-Unterstützung

Smartcards erhöhen den Privatsphärenschutz auf ein Maximum, indem Sie Nutzern eine physische Zugriffskontrolle gewährleisten, die Sie wie einen Türschlüssel am Bund bei sich tragen können. Bei Enterprise-Einsätzen ermitteln wir für Ihre Betriebsstruktur die bestmögliche Lösung der automatisierten Nutzererkennung.

Service und Support direkt vom Hersteller

Support und Maintenance

Neben unserer IT-Sicherheits-Software erhalten Sie je nach erworbenem GnuPG VS-Desktop® Paket zusätzliche Service- und Supportleistungen:

- **Telefonischer Support**
  Unsere *„Enterprise-Paket“*-Kunden erhalten von uns unlimitierte telefonische Beratung durch die leitenden Entwickler. Kleingruppen von bis zu 25 Nutzer erhalten von uns 2 Std./ Monat telefonischen Support zu unseren normalen Reaktionszeiten[(1)].

- **Feature-Requests**
  In Ihrem Auftrag entwickeln und programmieren wir neue, individuelle Funktionen und Features.

- **PKI-Konzipierung**
  Wir konfigurieren Ihnen ein passendes und individuell auf die Bedürfnisse Ihrer Organisation abgestimmtes Konzept für OpenPGP und S/MIME.

- **Smartcard-Anbindung**
  Gerne ermitteln wir für Ihre Betriebsstruktur eine Lösung zur automatisierten Nutzererkennung.

- **Sicherheits- / Major-Updates**
  Wir garantieren Ihnen kontinuierliche Pflege und Wartung unserer Software durch die leitenden Maintainer.

Entwicklung individueller Software-Features

Telefonischer Support

Betriebsunterstützung

Kommunikationslösungen sind zumeist individuell – wollen Sie OpenPGP oder S/MIME verwenden? Haben Sie sogar bereits eine bestehende S/MIME Infrastruktur? Unsere kompetenten und erfahrenen Techniker haben Antworten auf Ihre Fragen und geben Ihnen Ratschläge, wie Sie Ihre Prozesse verbessern und automatisieren können.

[(1)] Kritisch = 8 Std. / Hoch = 16 Std. / Normal = 24 Std.

Unsere Schulungs- und Beratungsleistungen

Schulung und Beratung

Unabhängig vom Erwerb eines GnuPG VS-Desktop® Pakets bieten wir Ihnen auf Wunsch auch weitere Beratungs- und Schulungsleistungen an:

- **Know-How**
  Individuelle Beratungs- und Lösungskonzepte zur Unterstützung Ihrer Organisation oder Institution.

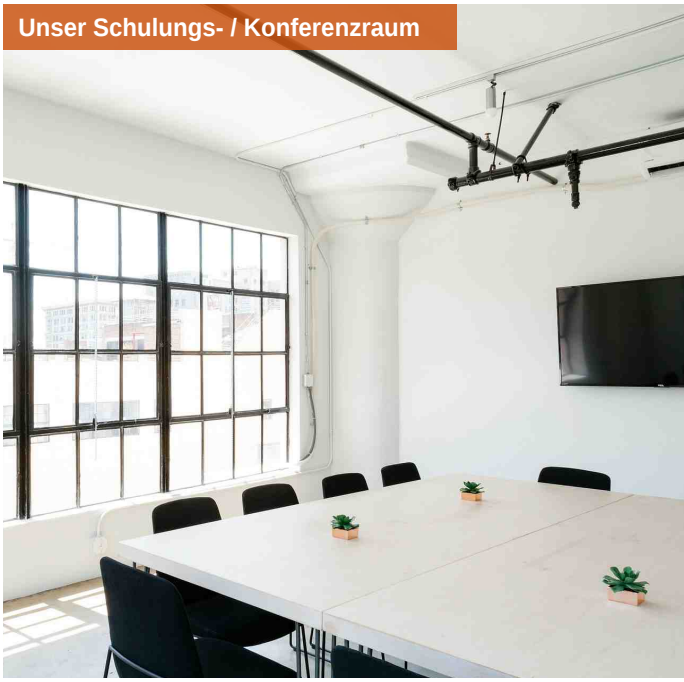
- **Einführung-Workshop**
  Im eintägigen Einführungs-Workshop vermitteln wir Ihrem IT-Sicherheitspersonal die Grundlagen der Ende-zu-Ende Verschlüsselung, analysieren die vorhandene Infrastruktur und erklären Ihnen, wie Sie unsere Software in Ihren Arbeitsalltag integrieren. Ebenso wie Sie Ihre Prozesse automatisieren und zentralisieren können.

- **Schulungsseminare**
  Maßgeschneiderte Seminare für Administratoren und IT-Sicherheitsbeauftragte zum sicheren Umgang mit unserer Software sowie zu den speziellen Anforderungen bei Verschlusssachen und SecOPs.

Seminar-Konfiguration
Unsere Kurse können von Ihnen bedarfsgerecht zu einem individuellen Seminar zusammengestellt werden

Unser Firmensitz in Erkrath bei Düsseldorf

Unser Schulungs- / Konferenzraum



Ihre Probleme – unsere Lösungen

Verschlüsselung wirkt auf den ersten Blick komplex. Dabei kann die Anwendung sehr einfach sein. Gerne beraten wir Ihre Administratoren und IT-Sicherheitsbeauftragten in den Themenfeldern Schlüssel-Management, Schlüssel-Verteilung und Prozessintegration.

Sie haben die Wahl – unsere Pakete im Überblick

Viel erwarten – mehr bekommen

Mit GnuPG VS-Desktop® erhalten Sie ein Komplettpaket aus IT-Sicherheits-Software, Beratung und telefonischen Support im Rahmen einer vertraglichen Vereinbarung. Wir haben für jeden unternehmerischen Einsatz eine passende Lösung:

GnuPG VS-Desktop®	Entry	Standard	Enterprise
Enthaltene Nutzer	–	25 Nutzer	250 Nutzer
Paketkonfiguration	standard	kundenspezifisch	kundenspezifisch
Dokumentationen	standard	standard	bedarfsoptimiert
Supportvolumen	1 Std. / Monat	2 Std. / Monat	unlimitiert
Technischer Support	✓	✓	✓
Bestandsanalyse	✗	✓	✓
Prozessbegleitung	✗	✗	✓
PKI-Konzipierung	✗	✓	✓
Feature-Requests	✗	✗	✓
Einführungs-Workshop	✗	✓	✓
VS-NfD Zulassung	✓	✓	✓
Major-Updates	✓	✓	✓
Weitergabe an Externe	✗	✓	✓

Bei dem Einsatz unserers *„Enterprise-Pakets“* haben Sie mit uns die Möglichkeit sich von uns zu überzeugen, indem Sie unser Software- und Dienstleistungsangebot bereits im Probebetrieb vollumfänglich testen. Sie erhalten von uns die notwendige Unterstützung bei der Installation, beim Rollout und bei der Anwendung.

Langjährig erprobte Kryptoagilität

Seit der Einführung von GnuPG in 1997 funktioniert unser Kryptocode stets sicher und zuverlässig. Unsere Software etablierte sich zur Standardlösung um Netzinfrastrukturen und -dienste abzusichern. Nahezu jeder Linux-Server nutzt heute das GnuPG-Verschlüsselungsverfahren um die Systemintegrität abzusichern.

Technische Daten und Systemanforderungen

GnuPG VS-Desktop®	
Datenverschlüsselung	OpenPGP | S/MIME | Symmetrisch
Mailverschlüsselung	PGP/MIME | S/MIME
Autom. Schlüsselabruf	OpenPGP über Web Key Directory | S/MIME über Zertifikatsserver
Vertrauensmodelle	Direkt | WoT (Web of Trust) | TOFU+PGP (Trust on first use)
Authenticated Encryption	Nur in OpenPGP
VS-NfD (EU-RESTRICTED)	S/MIME mit Smartcard | OpenPGP und S/MIME ohne Smartcard [2]
VS-V (EU-CONFIDENTIAL)	Nach Bewertung durch das BSI
Compliance	de-vs | OpenPGP | RFC4880bis | PGP6 | PGP7 | PGP8 | RFC2440
Unterstützte Smartcards	OpenPGP | NetKey | Yubikey | NitroKey | Gnuk | PKCS#15 | SC-HSM
ECC-Unterstützung für OpenPGP	Brainpool | NIST-P | Curve25519 | Bitcoin
Zufallsgeneratoren	CSPRNG (DRG.3) mit Jitter-RNG [3] | RDRAND | Padlock
Algorithmen	AES | Twofish | Camellia | SHA-256 | SHA-512 | RSA (bis 8192) | EdDSA | ECDH | ECDSA | DSA (deterministisch RFC6979)
Webbrowser (PKCS#11)	Hardware- und Software-Token (Firefox,Thunderbird etc.)
Webbrowser (WebMail)	Firefox | Chrome (z.B. mit Mailvelope)
Authentifizierung	Hardware- und Software-Token (SSH und PAM)

GpgOL Outlook-PlugIn	
Adressbuch-Integration	Festlegen und Verteilen der Schlüssel über das Adressbuch
Autocrypt-Unterstützung	Optional lesend. Inkl. verschlüsseltem Betreff
EFAIL-Schutz	Authenticated Encryption für OpenPGP | Absicherung für S/MIME
Nachrichtenleiste	Direktes Entschlüsseln ohne Interaktion
Inline-Editoren	Schnelles Antworten und Weiterleiten
Kompatibilitätsmodi	PGP/Inline
Phishing-Schutz	Über unterschiedliche Vertrauensstufen
Server	Microsoft Exchange (ab Version 2010) | IMAP
Verschlüsselte Entwürfe	OpenPGP | S/MIME

Systemanforderungen

GnuPG VS-Desktop® unterstützt 32- und 64bit-Windows-Systeme ab Version 7 oder neuer. GpgOL ist kompatibel mit Outlook 2010, 2013, 2016 und 2019 und unterstützt Mailtransport per SMTP / IMAP und Exchange Server ab 2010.

[2] Voraussetzung hierfür sind zusätzliche Schutzmaßnahmen, siehe VSA-BSI-10503
[3] Kein Einsatz des Windows-Zufallsgenerators

IT – Sicherheit

Made in Germany

g10 Code GmbH

Gutenbergweg 4
40699 Erkrath / Germany
+49 2104 493 879 0
info@gnupg.com
www.gnupg.com